Kali Linux

- Gebaut für die Durchführung von Penetrationtests und Offensive Security
- Zahlreiche Tools vorhanden um Systeme anzugreifen
  - Nutzen gute und böse Personen (Schwachstellen aufdecken oder Missbrauch)
- In der Regel eine VM, Windows Subsystem for Linux hat mittlerweile auch eine Version

Tools

- aircrack-ng: WLAN Passwörter knacken
- Burp suite: Proxy zum Client und Server (Web) App Security - Anfragen manipulieren
- OWASP-ZAP: Web App Scanner
- Nmap, Wireshark: Netzwerk-Analyse
- Nessus: Schwachstellenscanner - gibt Gesamtbild über ein System ob etwas angreifbar ist (z.B. Datenbank)
- SQLmap: SQL Injection (vor allem Webseiten)
  - xkcd - Comic zur SQL Injection https://xkcd.com/327/

SQLMap

- **Erkennung von SQL-Injection-Schwachstellen:** Sqlmap kann automatisch Schwachstellen in Webanwendungen erkennen, indem es verschiedene Arten von SQL-Injection-Angriffen testet.
- **Ausnutzen von SQL-Injection-Schwachstellen:** Sobald eine Schwachstelle gefunden wurde, kann sqlmap diese ausnutzen, um auf die zugrunde liegende Datenbank zuzugreifen.
- **Datenbank-Interaktion:** Sqlmap bietet eine Vielzahl von Funktionen zur Interaktion mit der Datenbank, wie z.B. das Abrufen von Tabellen- und Spaltennamen, das Auslesen von Daten, das Ausführen von SQL-Befehlen und sogar das Hoch- und Herunterladen von Dateien.
- **Umfangreiche Datenbankunterstützung:** Sqlmap unterstützt eine Vielzahl von Datenbankmanagementsystemen, darunter MySQL, PostgreSQL, Microsoft SQL Server, Oracle und viele andere.

Webseite testen:

- Auf SQL-Injection-Schwachstellen scannen falls vorhanden und Namen der Datenbanken auflisten

```
sqlmap -u "http://192.168.108.129/" --dbs
```

- Scan mit Post-Daten
  - Befehl sendet POST-Daten an die URL `login.php`

```
sqlmap -u "http://192.168.108.129/login.php" --data="username=test&password=test" --dbs
```

- Scan mit Cookies
  - Befehl beinhaltet Cookies, die für den Zugriff auf die Seite erforderlich sein könnten. Ersetzen von `PHPSESSID=12345` durch die tatsächlichen Cookies

```
sqlmap -u "http://192.168.108.129/" --cookie="PHPSESSID=12345" --dbs
```

Log-Dateien ansehen:

- Liegen beim Webserver im /var/log/apache2/access.log
  - Zugriffe von SQLmap werden hier sichtbar

Revision #8
Created 6 September 2024 06:45:58 by Max
Updated 6 September 2024 07:54:08 by Max